DIGITAL FORENSIC EXAMINATION NOTES

Date/Time	Action	Result
25 Apr 11, 1000	Consolidated and edited keyword list for maximum search coverage/efficiency	183 keywords
1200	Transferred images and keyword files to forensic machine using MicroForensics Evidence Mover v1.1.17	Transfers successful
26 Apr 11, 0730	Prepped forensic machine for operations	Successfully updated Symantec Endpoint Protection and Windows Defender. Windows not updated at this time due to internal network being down. Lack of windows updates will not adversely affect this examination.
0910	Conducted full AVS scan of forensic machine with Symantec Endpoint Protection v11.0.6100.645 (Def: April 25, 2011 r2)	No potential threats identified.
1433	Ensured all HOUSE media properly added to EnCase case file (0018-11-CID361_HOUSE.case)	Added USB storage key image, 8gb sd card image, HOUSE's netbook image, and contents of cell phone dump (as single files)
1437	Ran automated EnCase search for email	None found
1438	Ran EnCase condition to located potential email archive files (.PST, .OST, .MBOX, .EDB)	No email located
1443	Ran EnCase "File Mounter" enscript to mount identified compound files by file extension	File Mounter EnScript Started Processing 882 Files 77 file(s) mounted File Mounter EnScript completed in 234 Seconds
1445	Added keyword list to EnCase and set proper GREP flags where applicable, and made additional edits	N/A

Case# [redacted]
Evidence Tag# N/A
Examiner: [redacted]
Subject/Evidence Description: Data seized by ICE from HOUSE and [redacted] **at the U.S. Border**

Initials [redacted]

1455	Exported keywords	Successful
1457	Began hash analysis of all files in case using "Hash Set – NIST" and USACIL→"5-NSRL" hashsets to identify known files	Status: Completed Start: 26-Apr-11 15:53:35 Stop: 26-Apr-11 16:02:22 Time: 0:08:47 Files: 337,376 Hash values: 337,187
27 Apr 11, 0654	Ran "Fast Find Unique Files by Hash" EnCase filter. Sorted by "Hash Category" to eliminate "Known" system files from search.	106638 unique files of 337376 total files remained after filter. 103390 files remaining after selection of unique non-"Known" files
0700	Searched remaining unique files for keywords through "B" (38 total)	Status: Completed Start: 27-Apr-11 07:05:57 Stop: 27-Apr-11 07:55:59 Time: 0:50:02 Files: 103,390 Records: 0 Search Hits: 80,245 Added Search Hits: 80,234
0800	Searched remaining unique files for keywords from "D" through "G" (42 total)	Status: Completed Start: 27-Apr-11 08:01:50 Stop: 27-Apr-11 08:34:27 Time: 0:32:37 Files: 103,390 Records: 0 Search Hits: 125,796 Added Search Hits: 125,781
0906	Searched remaining unique files for keywords from "H" through "M" (43 total)	Status: Completed Start: 27-Apr-11 09:07:35 Stop: 27-Apr-11 09:21:04

Case# [redacted]
Evidence Tag# N/A
Examiner: [redacted]
Subject/Evidence Description: Data seized by ICE from HOUSE and [redacted] **at the U.S. Border**

		Time: 0:13:29 Files: 103,390 Records: 0 Search Hits: 73,992 Added Search Hits: 73,992
1005	Searched remaining unique files for keywords from "N" through "Z" (60 total)	Status: Completed Start: 27-Apr-11 10:05:16 Stop: 27-Apr-11 10:20:49 Time: 0:15:33 Files: 103,390 Records: 0 Search Hits: 247,703 Added Search Hits: 246,278
1230	Ran "Show one hit per file" filter	26,148 total files/objects identified as potentially responsive to the keyword list
[redacted]		
1322	Ran automated EnCase search for email	Identified 802608 email objects displayed in the EnCase records view. Due to pathing issues, will keyword search email messages in EnCase instead of exporting.
1445	Ran EnCase "File Mounter" enscript to mount identified compound files by file extension, excluding email data (total: 1451279 files)	File Mounter EnScript Started Processing 27614 Files 23394 file(s) mounted File Mounter EnScript completed in 432 Seconds
1500	[redacted]	N/A

Case# [redacted]
Evidence Tag# N/A
Examiner: [redacted]
Subject/Evidence Description: Data seized by ICE from HOUSE and [redacted] **at the U.S. Border**

	[redacted]	
1505	Began hash analysis of all files in case using "Hash Set – NIST" and USACIL→"5-NSRL" hashsets to identify known files	Status: Completed Start: 27-Apr-11 15:05:58 Stop: 27-Apr-11 15:28:42 Time: 0:22:44 Files: 2,254,833 Hash values: 2,004,231
28 April 11 – 4 May 11	Examiner on bereavement leave	
[redacted]		
1246	Examined keyword hits for HOUSE USB Key Storage device	Nothing of evidentiary value found.
1313	Examined keyword hits for HOUSE 8gb SD Card	Nothing of evidentiary value found. Device appears to have been encrypted with unknown technique/tool.
1315	Examined keyword hits for HOUSE UFED (Single Files) data	9 potentially pertinent files located and bookmarked
[redacted]		
1355	Began examination of keyword hits for HOUSE Netbook	Finished " M " through "Attorney". 1 potentially pertinent file identified and

		bookmarked.
[redacted]		
1300	Continued examination of keyword hits for HOUSE Netbook.	Completed list. 33 potentially pertinent files identified and bookmarked.
1500	Pertinent bookmarked files from HOUSE media reviewed by [redacted]	No pertinent data that would justify seizure by ICE.
[redacted]		

[redacted]

Case# [redacted]
Evidence Tag# N/A
Examiner: [redacted]
Subject/Evidence Description: Data seized by ICE from HOUSE and [redacted] at the U.S. Border

[redacted]

Case# [redacted]
Evidence Tag# N/A
Examiner: [redacted]
Subject/Evidence Description: Data seized by ICE from HOUSE and [redacted] at the U.S. Border

Initials [redacted]

[redacted]

Case# [redacted]
Evidence Tag# N/A
Examiner: [redacted]
Subject/Evidence Description: Data seized by ICE from HOUSE and [redacted] at the U.S. Border

[redacted]

Case# [redacted]
Evidence Tag# N/A
Examiner: [redacted]
Subject/Evidence Description: Data seized by ICE from HOUSE and [redacted] at the U.S. Border

[redacted]

Case# [redacted]
Evidence Tag# N/A
Examiner: [redacted]
Subject/Evidence Description: Data seized by ICE from HOUSE and [redacted] at the U.S. Border

Initials [redacted]

	needed for meeting with ICE at 1400. Just description of what, if anything, was found during the examinations.	
1400	Meeting with ICE	Demand Letter satisfied. Request to delete case data. Examination terminated.